

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1]A telephone network terminal accommodated in a telephone network and a computer terminal accommodated in a computer network, In a method of attesting an addresser at the time of communicating a message via intermediate equipment (it is only described as intermediate equipment below) with the above-mentioned telephone network, each of the above-mentioned computer network, and an interface, An addresser authentication method attesting a signature of a message which attached to the message a digital signature of an addresser who uses the computer terminal, transmitted to it, and received with the above-mentioned intermediate equipment when sending a message from the above-mentioned computer terminal.

[Claim 2]The addresser authentication method according to claim 1 comparing a sender number which memorized [above-mentioned] the sender number, and attesting intermediate equipment if a sender number of the above-mentioned intermediate equipment is memorized to the above-mentioned telephone network terminal and the above-mentioned telephone network terminal has needed information from the above-mentioned intermediate equipment.

[Claim 3]The addresser authentication method according to claim 2 if the above-mentioned telephone network terminal passes [collation of the above-mentioned sender number], wherein it will attest an addresser by originator information of the above-mentioned computer terminal notified with a message from the above-mentioned intermediate equipment.

[Claim 4]Memorize message ID of a message which received to the above-mentioned intermediate equipment, and the above-mentioned computer terminal gives message ID to the outgoing message, If the above-mentioned digital signature is performed also to this message ID and the above-mentioned intermediate equipment is in agreement as compared with the above-mentioned message ID which memorized message ID in a message from the above-mentioned computer terminal before it, The addresser authentication method according to any

one of claims 1 to 3 processing as an illegal message.

[Claim 5]A telephone network terminal accommodated in a telephone network and a computer terminal accommodated in a computer network, In a method of attesting an addresser at the time of communicating a message via intermediate equipment (it is only described as intermediate equipment below) with the above-mentioned telephone network, each of the above-mentioned computer network, and an interface, An addresser authentication method, wherein the above-mentioned intermediate equipment attaches a digital signature of intermediate equipment to this, and transmits a message which received from the above-mentioned telephone network terminal to the above-mentioned computer terminal and the above-mentioned computer terminal attests a signature of a message which received.

[Claim 6]The addresser authentication method according to claim 5 comparing with a sender number which memorized [above-mentioned] the sender number, and attesting an addresser if a sender number of the above-mentioned telephone network terminal is memorized to the above-mentioned intermediate equipment and the above-mentioned intermediate equipment has the needed information from the above-mentioned telephone network terminal.

[Claim 7]The addresser authentication method according to claim 5 or 6 attesting an addresser by originator information of the above-mentioned telephone network terminal notified with a message from the above-mentioned intermediate equipment if attestation of a signature of the above-mentioned message is passed.

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention relates to an addresser's authentication method in the communication which performs message communication mutually between the terminals of a computer network and a telephone network.

[0002]

[Description of the Prior Art]The intermediate equipment (it is only described as intermediate equipment below) 13 which has an interface in each of the public telephone network 11 and the computer network 12 as shown in drawing 12 is formed, The correspondence procedure with which the telephone network terminal 14 accommodated in the telephone network 11 and the computer terminal 15 accommodated in the computer network 12 communicate a message via the intermediate equipment 13 is known.

[0003]Conventionally, with the service which performs message communication mutually, the following two methods are mainly taken as a method of performing addresser attestation for fee collection etc., according to the purpose between the terminals 15 and 14 of such a computer network 12 and the telephone network 11. When registering an e-mail address into the intermediate equipment 13 beforehand and transmitting the E-mail from the computer network 12 side to the facsimile terminal 14 as a telephone network terminal via the intermediate equipment 13, the 1st method, If an E-mail is sent to the intermediate equipment 13 from the dispatch computer terminal 15 as shown in drawing 1, The intermediate equipment 13 performs addresser attestation by comparing with the e-mail address which registered beforehand the mail address of the master station 15 in an E-mail, If the attestation is passed, messages, such as a text (character) in the E-mail received from the computer terminal 15 and a picture, will be changed into a facsimile signal, that is, media conversion is performed, and it transmits to the facsimile terminal 14 of a telephone network to a destination side. If the

facsimile terminal 14 has mail arrival via the intermediate equipment 13, the addressee of the facsimile terminal 14 will check an addresser by said e-mail address attached to the message in the reproduced image of the facsimile terminal 14.

[0004]In [when transmitting a facsimile to the computer terminal 15 from the telephone network terminal 14 side, as it is shown in drawing 2] the intermediate equipment 13, Addresser attestation is not performed [as opposed to / especially / the facsimile received from the terminal 14], but media conversion of the facsimile signal is carried out to the form of an E-mail, and it transmits to the computer terminal 15 of a destination side. The addressee of the computer terminal 15 who received this E-mail checks an addresser by the cover page which the addresser of the terminal 14 added.

[0005]The 2nd method registers ID (user identification information) and the password for attesting an addresser into the intermediate equipment 13 beforehand, When transmitting the E-mail from the computer network 12 side to the facsimile terminal 14 of the telephone network 11 via the intermediate equipment 13, As shown in drawing 3, ID and the password for attesting an addresser with the dispatch computer terminal 15 are attached to an E-mail, Transmit an E-mail to the intermediate equipment 13, and the intermediate equipment 13 performs addresser attestation by comparing with ID in the received E-mail, ID which registered the password beforehand, and a password, If attestation is passed, the message of the E-mail will be changed into a facsimile signal, and it will transmit to the facsimile terminal 14 of a telephone network. The addressee of the facsimile terminal 14 checks an addresser by an addresser's ID added to the reproduced image message of the facsimile terminal 14.

[0006]When transmitting a facsimile to the computer terminal 15 from the telephone network 11 side, As shown in drawing 4, ID and a password for an addresser to attest an addresser to PB sound are entered from the facsimile terminal 14, If the intermediate equipment 13 performs addresser attestation and passes this by comparing with the inputted ID, ID which registered the password beforehand, and a password, it will change into an E-mail the facsimile sent after that, and will transmit to the computer terminal 15. The addressee of the computer terminal 15 checks an addresser by addresser ID added to the message of the E-mail which received.

[0007]

[Problem(s) to be Solved by the Invention]In the 1st conventional method, when an addresser's e-mail address is revealed, he is able for the 3rd person to camouflage an addresser's e-mail address unjustly, and to transmit a message, and it may become disadvantageous to an addresser and an addressee. The 3rd person altered unjustly the message which the addresser transmitted, and there was a problem that it may become disadvantageous to an addresser and an addressee. When transmitting a facsimile to a computer terminal from the telephone network 11, in order not to attest with the intermediate

equipment 13, When the 3rd person transmitted a facsimile unjustly, there was a problem that there was a possibility of becoming an addressee's disadvantage, by transmitting to an addressee the message which there is a possibility of bringing the administrator of the intermediate equipment 13 a disadvantage, and an addresser cannot specify.

[0008]In the 2nd conventional method, he is able for the 3rd person to camouflage an addresser's ID and password unjustly, and to transmit a message like the 1st conventional method, and it may become disadvantageous to an addresser and an addressee. The 3rd person altered unjustly the message which the addresser transmitted, and there was a problem that it may become disadvantageous to an addresser and an addressee. Also when ****(ing) a facsimile from the telephone network 11 to the computer terminal 15, there was a problem that he was able for the 3rd person to do camouflage use of an addresser's ID and password unjustly, and to transmit a message, and it may become disadvantageous to an addresser and an addressee.

[0009]. Solved the problem that this invention became a disadvantage of the administrator of intermediate equipment when the 3rd person turns into an addresser, it clears up, or the 3rd person alters a message and the problem and the 3rd person of an addresser and an addressee of becoming a disadvantage transmit a facsimile unjustly. It aims at proposing an addresser authentication method.

[0010]

[Means for Solving the Problem]It is this invention performing a digital signature, when sending from a computer terminal, and performing addresser attestation using a digital signature added to a message with intermediate equipment, It is performing addresser attestation using a sender number which enables detection of an alteration to prevention and a message of spoofing by the 3rd person, and is notified from a telephone network to dispatch [terminal / telephone network], If prevention of spoofing by the 3rd person is enabled and a telephone network terminal has mail arrival, The addressee enables an addresser's check by performing addresser attestation using a sender number of intermediate equipment notified from the intermediate equipment 13, and originator information in an incoming message, If a computer terminal has mail arrival, the addressee attests intermediate equipment using a digital signature of intermediate equipment added to an incoming message, will be taking out originator information in a message, and will enable an addresser's check.

[0011]

[Function]As opposed to the addresser connected to the computer network in attestation with intermediate equipment, By performing addresser attestation using the digital signature added to the message, if digital signatures differ even if the 3rd person fakes an addresser's e-mail address, it can cancel as an inaccurate message. Since only an addresser can create a digital signature and it differs for every message, it becomes possible to detect, even if it is a case

where a part of message is altered when the 3rd person reproduces a digital signature unjustly and. By giving a digital signature also to the message ID given to a meaning by an electronic mail device, by canceling a message with the same message ID, even if it is a case where the whole message is reproduced unjustly, it becomes detectable. To the addresser connected to the telephone network, it is not from an addresser, but is performing addresser attestation using the sender number notified from a telephone network, and it becomes possible to prevent the 3rd person becoming completely unjustly. The addressee connected to the telephone network also in attestation by an addressee, An addresser's check is attained by performing addresser attestation by acquiring only the sender number of intermediate equipment beforehand using the sender number of the intermediate equipment notified from a telephone network, and the originator information in a message, It is acquiring only the public key of intermediate equipment beforehand, and the addressee connected to the computer network attests intermediate equipment using the digital signature of intermediate equipment, he is taking out the originator information in a message, and an addresser's check of him is attained.

[0012]

[Embodiment of the Invention]

An example of the communications system with which this invention is applied to example 1 drawing 1 A is shown, and identical codes are attached to drawing 12 and a corresponding portion. The telephone network 11 is provided with the sender number reporting means 21. The telephone network terminal 14 is provided with the communication control means 22 which sends and receives a signal with the telephone network 11, In this example, it is a case of a facsimile terminal, and it had the image input output means 23, and has further the sender number extraction means 24 and also the accumulation means 25 which memorizes the sender number of the intermediate equipment 13 from the incoming message in this invention.

[0013]The intermediate equipment 13 is provided with the telephone network 11, and the computer network 12 and the communication control means (interface) 26 and 27 which send and receive communication, respectively, and also in this invention. It has the accumulation means 32 which memorizes the sender number extraction means 28, a means 29 to add a digital signature to an outgoing message, the media conversion means 30, the means 31 that compares a receiving digital signature (verification), a public key still more nearly required for a digital signature and its verification, and a secret key.

[0014]The computer terminal 15 is provided with the communication control means 33 which sends and receives communication with the computer network 12, and the input output means 34 of an E-mail, and also. In this invention, it has the accumulation means 37 which memorizes a means 35 to add a digital signature to an outgoing message, the means 36 which compares a receiving digital signature (verification), a digital signature, a public key required

for that verification, and a secret key.

[0015]Although a digital signature is used in this invention, acquisition of the key needed for this is explained with reference to drawing 2. The intermediate equipment 13 generates the pair of a public key and a secret key, registers a public key into the certificate authority 39, and it memorizes a secret key to the accumulation means 32. The computer terminal 15 acquires the public key of the intermediate equipment 13 from the certificate authority 39, Generate the pair of a public key and a secret key, register the public key into the certificate authority 39, memorize a secret key to the accumulation means 37, and also a digital signature is attached with the secret key of the computer terminal 15 to user's information (ID), such as a self name, This is enciphered by the public key of the intermediate equipment 13, and it transmits to the intermediate equipment 13. The intermediate equipment 13 decrypts those received data with the secret key of the intermediate equipment 13, and acquire the public key of the computer terminal 15 from the certificate authority 39, verify said decryption digital signature by this public key, and if it passes, Carry out accumulation registration of the user's information of the received computer terminal 15 which was decrypted at the accumulation means 32, and the message which shows the registration result is created, On the other hand, it signs with the secret key of the intermediate equipment 13, the registration result message with a signature is enciphered by the public key of the computer terminal 15, and it transmits to the computer terminal 15. The computer terminal 15 decrypts the received encryption data with a secret key, verifies the decrypted signature by the public key of the intermediate equipment 13, and checks the contents of registration.

[0016]This Example 1 is a case where a message is transmitted from the computer terminal 15 to the telephone network terminal 14 via the intermediate equipment 13. In this case, the addresser who uses the electronic mail device (computer terminal) 15 beforehand by for example, the method explained by drawing 2. The subscriber information of the addresser (computer terminal 15) who is information required for attestation is registered into the subscriber information accumulation means 32 in the intermediate equipment 13, The intermediate equipment 13 acquires the public key of the computer terminal 15 required for an addresser's attestation, The addressee who memorizes and uses a facsimile terminal for the subscriber information accumulation means 32 in the telephone network terminal 14 and this example accumulates the sender number of the intermediate equipment 13 required for attestation of the intermediate equipment 13 in the information accumulation means 22 beforehand.

[0017]When transmitting a message from the computer terminal 15, a message is created by the e-mail input output means 34, by the digital signature addition means 35, to said created message, the secret key of the computer terminal 15 is used and an addresser's digital signature is added. The message which added this digital signature is transmitted by the

communication control means 33 to the intermediate equipment 13.

[0018]The intermediate equipment 13 receives this message from the communication control means 27, uses the public key of the computer terminal 15 beforehand accumulated in the accumulation means 32 by the digital signature collation means 31, and compares the digital signature added to the message. As a result of comparing, when a digital signature belongs to an addresser to be sure and it is not altered, it is interpreted as it being a right message, and the contents of the E-mail are changed into a facsimile image by the media conversion means 30. A message is canceled when a digital signature is inaccurate. The message which performed media conversion is transmitted by the communication control means 26 to the telephone network terminal 14. If the call origination to the telephone network terminal 14 occurs from the intermediate equipment 13, the telephone network 11 will notify the sender number of the intermediate equipment 13 to the receiving terminal 14 by the originator information reporting means 21. The receiving terminal 14 extracts a sender number by the sender number extraction means 24, and after checking that it is the receipt from the intermediate equipment 13 with the sender number of the intermediate equipment 13 accumulated in the information accumulation means 25, the communication control means 22 receives a facsimile. Since the addresser's information is added, the reproduced image of the received facsimile can check that an addresser is an addresser registered into the intermediate equipment 13.

[0019]It seems that the E-mail created with the computer terminal 15 is shown in drawing 3. Namely, the addresser address 61 is described first and the format 62 (this example MIME version 1.0) of the following description is shown below, It is described that the partner point (addressee) address 63 is [the theme 64] a test in the Japanese JIS code in this example following this, Next, the inner form 65 shows a boundary by a multi-part/mixing in this example at "... 742959F6218E", After attaching this boundary 66, and it usually being shown for the inner form 67 by this example a text / that a character is a JIS code and also showing that the contents conversion coding 68 is 7-bit numerals in this example, the text 69 which is a message content is described. It is shown behind the next boundary 70 that the inner form 71 is a picture in this example, and that format is gif, it is shown that that contents conversion coding 72 is based on base64 in this example, that coded image data 73 is described below, and the boundary 74 is attached that end.

[0020]The E-mail which signed to this message comes to be shown in drawing 4. That is, the origination address 61, the description format 62, the mail arrival address 63, and the theme 64 are the same as that of drawing 3, and it is the following inner form 65, Become a multi-part and with a signature and a boundary is set to "Next Part Level-1-152633", After it is described that a signature algorithm is pgp-md5 and that it is a message in the next inner form 67 of the boundary 66 and its format rfc822 are described, The description 75 of all the messages in

drawing 3 is made, it is the signature by the pgp method, the signature data 78 follows the inner form 77 following the boundary 76 of the end, and, finally the boundary 79 is attached to it.

[0021]By the media conversion means 30 in the intermediate equipment 13, in this example, the text (character) 69 in an incoming message is changed into the data of a facsimile image as shown in drawing 5, and as the picture message 73 is also shown in drawing 5, it is changed into the data of a facsimile image. In this case, an addresser address and the theme are added to the upper left end of both screens as image data.

[0022]The flow of processing of the example mentioned above is shown in drawing 6. In the computer terminal 15, to the created message, it signs with the secret key of the terminal 15, and sends to the intermediate equipment 13 by making this message with a signature into an E-mail. If a signature is verified and it passes by the public key of the terminal 15, media conversion of the message will be carried out, the telephone network terminal (facsimile terminal) 14 will be called, the terminal 14 checks the sender number of the intermediate equipment 13, and if the intermediate equipment 13 is right, it will answer the intermediate equipment 13 and will receive a facsimile. From the origination address in the reproduced image of the facsimile, it checks being sent from the addresser 15, i.e., a computer terminal. The example of this invention is shown in example 2 drawing 7. This is a case where a message is transmitted to the computer terminal 15 via the intermediate equipment 13 from the telephone network terminal 14.

[0023]The addresser who uses the facsimile terminal 14 as a telephone network terminal registers his sender number with the subscriber information accumulation means 32 in the intermediate equipment 13 beforehand. [required for attestation]The addressee who uses the electronic mail device 15 of a computer terminal acquires the public key of intermediate equipment required for attestation of the intermediate equipment 13 from a certificate authority, and accumulates in the information accumulation means 37. When transmitting a message to the computer terminal 15 from the facsimile terminal 14, a facsimile image as shown in drawing 8 by the facsimile input output means 23 is inputted. The inputted facsimile image is transmitted by the communication control means 22 to the intermediate equipment 13. If call origination occurs from the terminal 14 to the intermediate equipment 13 in that case, the telephone network 11 will notify the sender number of the master station 14 to the intermediate equipment 13 by the originator information reporting means 21. By the sender number extraction means 28, after the intermediate equipment 13 extracts the sender number of a master station, it is compared with the sender number of the terminal 14 accumulated in the subscriber information accumulation means 32. In a right case, by the communication control means 26, the compared result receives a facsimile. When a sender number is not in agreement, it is judged as unjust receipt, and it does not receive. The received facsimile image

is changed into the format of an E-mail as shown in drawing 9 by the media conversion means 30. This E-mail is the origination address 61, the description format 62, the recipient address 63, and the theme 64 (this example FAX) like the case of drawing 3, and that to which the next of the boundary 66 after the inner form 65 was described corresponded with the picture message part in drawing 3 continues.

[0024]The message changed into this electronic mail format adds the digital signature of the intermediate equipment 13 like the case where it is shown in drawing 4, by the digital signature addition means 29. The message which added the digital signature is transmitted to the computer terminal (electronic mail device) 15 by the communication control means 27. After the computer terminal 15 receives a message by the communication control means 33, it uses the public key of the intermediate equipment 13 acquired beforehand for the information accumulation means 37 by the digital signature collation means 36, and compares the digital signature added to the message. If the compared result is right, it can check that an addresser is an addresser registered into the intermediate equipment 13 by the originator information (address) indicated in the From line in the E-mail.

Example 3 -- the difference from Example 1 by the case where this example transmits a message from the computer terminal 15 to the telephone network terminal 14 via the intermediate equipment 13, A digital signature is not given only to the message which the addresser created, A digital signature is given also to the message ID added by the communication control means 33 in the computer terminal 15, it is lost by this that message ID is altered, and it makes it possible to identify a message uniquely by message ID. In order to realize this, it provides, as the ID accumulation means 41 which memorizes the message ID which received in the intermediate equipment 13 shows drawing 1 as a solid line.

[0025]This procedure is shown in drawing 10. The public key of the computer terminal 15 is registered into the intermediate equipment 13 like an example, and the sender number of the intermediate equipment 13 is accumulated in the information accumulation means 25 of the telephone network terminal 14. When transmitting a message from the computer terminal 15, a message is created by the input output means 34, and message ID is added by the communication control means 33 to this message. By the digital signature addition means 35, its digital signature is added to said message, and it transmits to the intermediate equipment 13 by the communication control means 33.

[0026]The user's information beforehand accumulated in the accumulation means 32 is used for the intermediate equipment 13 which received the message by the digital signature collation means 31, and it compares the digital signature added to the message. A message is canceled when a digital signature is inaccurate. As a result of comparing, when a digital signature belongs to an addresser to be sure and it is not altered, it is interpreted as it being a right message, and comparison with all the message ID accumulated in the ID accumulation

means 41 next and the message ID in an incoming message is performed. When message ID differs, the message ID in a message is accumulated in the ID accumulation means 41, and it changes into the data of a facsimile image as showed drawing 5 the contents of the E-mail by the media conversion means 30. When that message ID already exists in the message ID accumulation means 41 as a result of comparison of said message ID, this incoming message judges it as what was reproduced unjustly, and cancels that message. The message which performed media conversion transmits to a facsimile terminal with the telephone network terminal 14 by the communication control means 26. Next processing is the same as that of Example 1.

[0027]It may carry out, as shown in drawing 11 as an acquisition method of a public key. Like the case of drawing 2, the intermediate equipment 13 and the computer terminal 15 generate the pair of a public key and a secret key, respectively, and perform registration for a public key and their information to the certificate authority 39, respectively. I have a certificate of acknowledgement in registration in that case published from the certificate authority 39, and the certificate is accumulated in the accumulation means 32 and 37, respectively. In order to register the user's information into the intermediate equipment 13, the computer terminal 15, if acquire the certificate of the intermediate equipment 13 to intermediate equipment first, and the public key of the certificate authority 39 to the certificate authority 39 is acquired, the certificate of the acquired intermediate equipment is attested using this public key and that attestation is passed, From the certificate, the public key of the intermediate equipment 13 is taken out, the user's information of the computer terminal 15 is enciphered by the public key, it signs by the confidential information of the computer terminal 15 to this, and the encryption user's information with a signature and the certificate of a computer terminal are transmitted to the intermediate equipment 13.

[0028]If the public key of the certificate authority 39 to a certificate authority is received, the certificate of the computer terminal received by this public key is attested in the intermediate equipment 13 and this is passed, If take out the public key of the computer terminal 15 from the certificate, and the public key is accumulated in the accumulation means 32, and the signature of the encryption user's information received by the public key is verified and this is passed, After decrypting the encryption user's information with the secret key of the intermediate equipment 13 and checking whether it is correct by the contents of the user's information, user's information is memorized to the accumulation means 32. The registration result message is enciphered by the public key of the computer terminal 15, and the signature of the intermediate equipment 13 is attached to this, and also the certificate of intermediate equipment is also attached, and the encryption registration result is sent to the computer terminal 15.

[0029]In a similar manner, the computer terminal 15 verifies the signature of a reception

registration result by the public key of intermediate equipment, further, is decrypted with the secret key of the computer terminal 15, and checks the contents of registration. Thus, if the certificate of the computer terminal 15 (intermediate equipment 13) is attached to the message which I get to publish a certificate and transmits from the computer terminal 15 (or intermediate equipment 13) and it transmits to it, The received intermediate equipment 13 (computer terminal 15) can obtain the public key of the computer terminal 15 (intermediate equipment 13) from the received certificate. Therefore, the intermediate equipment 13 does not need to acquire the public key of the computer terminal 15 from the certificate authority 39.

[0030]

[Effect of the Invention]In [according to / as explained above / the invention of claims 1 thru/or 4] registration of the message from the computer terminal 15, It becomes possible to become detectable [the alteration to the prevention and the message of spoofing by the 3rd person] with the intermediate equipment 13, and to detect the duplicate of the message by the 3rd person, and there is an economical effect that fee collection to an addresser is performed correctly.

[0031]According to the invention of claims 5 thru/or 7, in registration of the message from the telephone network terminal 14, prevention of spoofing by the 3rd person is attained with the intermediate equipment 13, and there is an economical effect that fee collection to an addresser is performed correctly. According to the invention of claim 2, in the addresser attestation in a receiving terminal, it is effective in an addresser raising the serviceability that the check in a right paddle is attained, only by acquiring the information on intermediate equipment beforehand.

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] The block diagram showing the example of the communications system with which this invention method is applied.

[Drawing 2] The figure showing the procedure of the public key acquisition method used for this invention.

[Drawing 3] The figure showing the example of the message made from the computer terminal 15.

[Drawing 4] The figure showing the example of the E-mail which carried out the digital signature of the message of drawing 3 with the computer terminal 15.

[Drawing 5] The figure showing the example which changed the message of drawing 3 into the facsimile image.

[Drawing 6] The figure showing the sequence of the example of an invention of claim 2.

[Drawing 7] The figure showing the sequence of the example of an invention of claim 5.

[Drawing 8] The figure showing the example of a transmitting facsimile image.

[Drawing 9] The figure showing the example which changed the facsimile image of drawing 8 into the electronic message.

[Drawing 10] The figure showing the sequence of the example of an invention of claim 4.

[Drawing 11] The figure showing the sequence of other methods of public key acquisition.

[Drawing 12] The figure showing the example of the communications system with which this invention method is applied.

[Drawing 13] The figure showing the sequence at the time of sending from the conventional telephone network terminal.

[Drawing 14] The figure showing the sequence at the time of sending from the conventional computer terminal.

[Drawing 15] The figure showing the sequence at the time of sending from the conventional

telephone network terminal.

[Drawing 16] The figure showing the sequence at the time of sending from the conventional computer terminal.

[Translation done.]

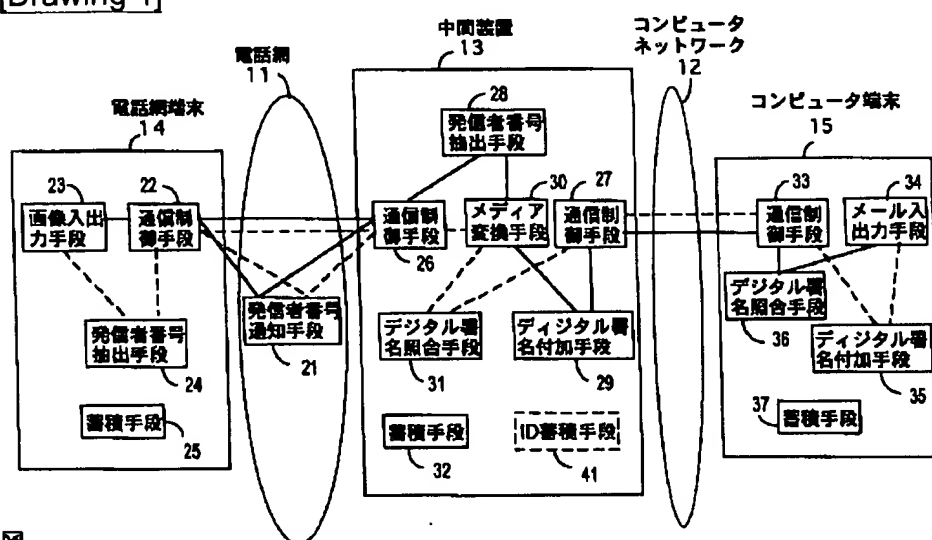
* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DRAWINGS

[Drawing 1]



図

[Drawing 6]

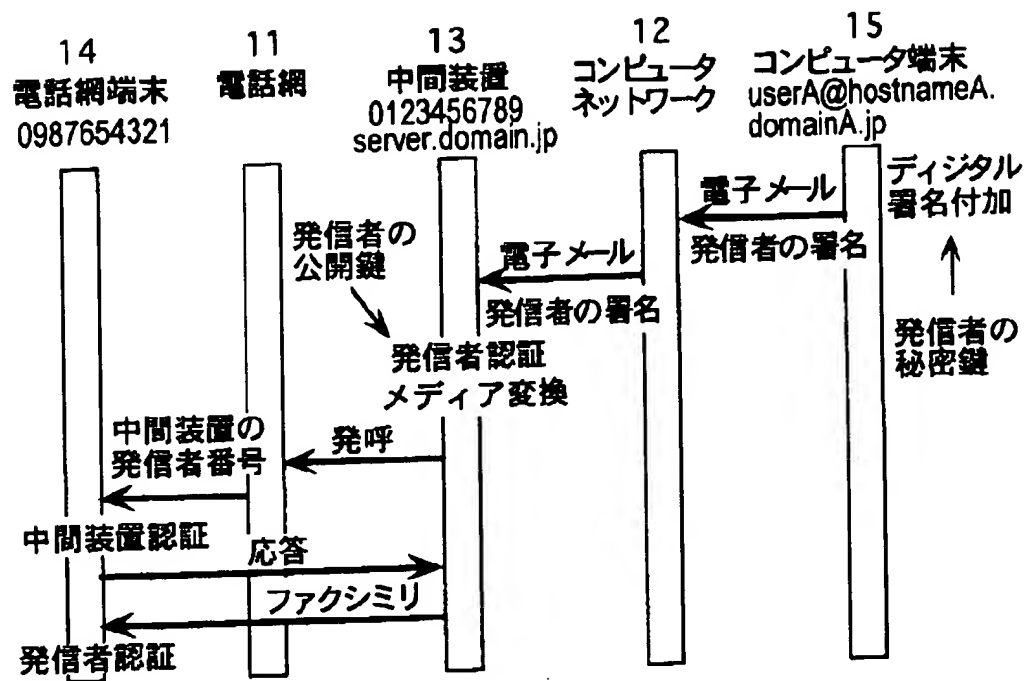


図 6

[Drawing 2]

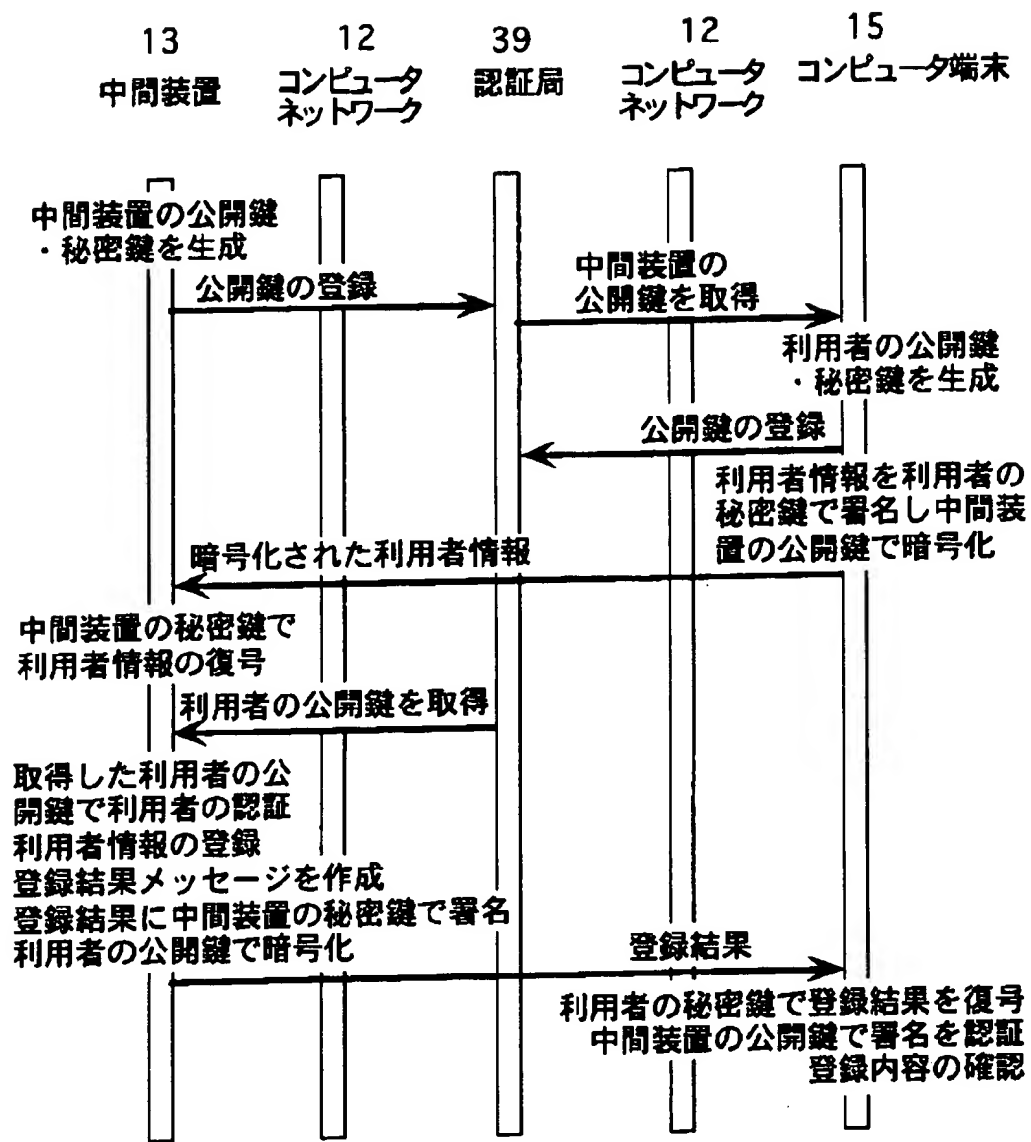


図 2

[Drawing 12]

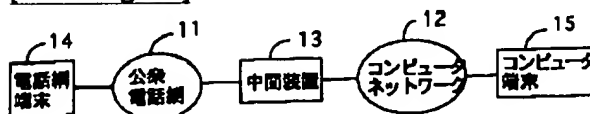


図12

[Drawing 3]

```

61 From: userA@hostnameA.domainA.jp
62 MIME-Version: 1.0
63 To: 0987654321@server.domain.jp
64 Subject: =?iso-2022-jp?B?GyRCJUYIOSVIGyhK?=?
65 Content-Type: multipart/mixed; boundary=".....742959F6218E"

```

This is a multi-part message in MIME format.

```

66 .....742959F6218E
67 Content-Type: text/plain; charset=iso-2022-jp
68 Content-Transfer-Encoding: 7bit

```

```

69 こんにちは。
    これはテストです。

```

```

70 .....742959F6218E
71 Content-Type: image/gif; name="sample.gif"
72 Content-Transfer-Encoding: base64

```

```

73 {
    R0KGODthawBaAPcAAP////Hu7Ofb0vIPqsDAwMXFxaG0k8uI
    KWlpYWFhXJpZFpaWKA/PJAwmBYVFQAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    <中略>
    mDXSW8oSTgCv5yQxPMZVzKId9AJFFgWaBTLXa5/7EPiWpURv
    R2PhV2dCiDziZHB7PeFg79Cifg3mxUfEa4vPcnIZdJQdr+hy7
    byAkHx0UhdFKTKDD33JerrZUf9epmWdykL4Lhryf8U56vIFg/
    kMVPpFczHMSaCDKC+MIRBYgbgRUGQX4D2QbCs92sBSzbpVm
    M607230gs8lqloQ+ajzJgkBEEx+QABjLkYwb988pIPvnxj4C8TUA
    AADs=

```

```

74 .....742959F6218E.....

```

図 3

[Drawing 4]

```

61 From: userA@hostnameA.domainA.jp
62 MIME-Version: 1.0
63 To: 0987654321@server.domain.jp
64 Subject: =?iso-2022-jp?B?GyRCJUyYlosvIGyhK?=
65 Content-Type: multipart/signed; boundary="Next_Part_Level_1_152633";
    micalg=pqpmid5;
    protocol="application/pgp-signature"

66 .....Next_Part_Level_1_152633
67 Content-Type: message/rfc822
    From: userA@hostnameA.domainA.jp
    MIME-Version: 1.0
    To: 0987654321@server.domain.jp
    Subject: =?iso-2022-jp?B?GyRCJUyYlosvIGyhK?=
    Content-Type: multipart/mixed; boundary=".....742959F6218E"
    This is a multi-part message in MIME format.
    .....742959F6218E
    Content-Type: text/plain; charset=iso-2022-jp
    Content-Transfer-Encoding: 7bit
75 こんにちは。
    これはテストです。
    .....742959F6218E
    Content-Type: image/gif; name="faximage1.gif"
    Content-Transfer-Encoding: base64
    Content-Disposition: inline; filename="faximage1.gif"
    R0lGODlhawBaAPcAAP///Hu7OfoDvfpqsDAwMXFxeG0k8ulKWlpYWFhXUpZ
    FpaWKA/PjAwMBYVFQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    <中略>
    IFgAMVPPFczHMSaCDKC+MRBYgbjRUGQXAD2QbCs92eBSzbpVmiM072
    3Ugs8lqloQ+ejzJgkBEr+0ABjLJkyw59jHPvnx4C8TUAAADs=
    .....742959F6218E.....
76 .....Next_Part_Level_1_1512633
77 Content-Type: application/pgp-signature
    .....BEGIN PGP SIGNATURE.....
    Version: 2.6.2
78 IQBVAwUBMyWlWw8FMT+s8tpAQFMCah/dOXF1AkhNPzayfItmD3kcowz59z
    n6KmlC2+uVJnCZnuZYxEEY4emq8lgDc9jwemXnfQ231EYHGNUHYRTZg=
    =g0b6
79 .....END PGP SIGNATURE.....
    .....Next_Part_Level_1_152633-

```

図 4

[Drawing 5]

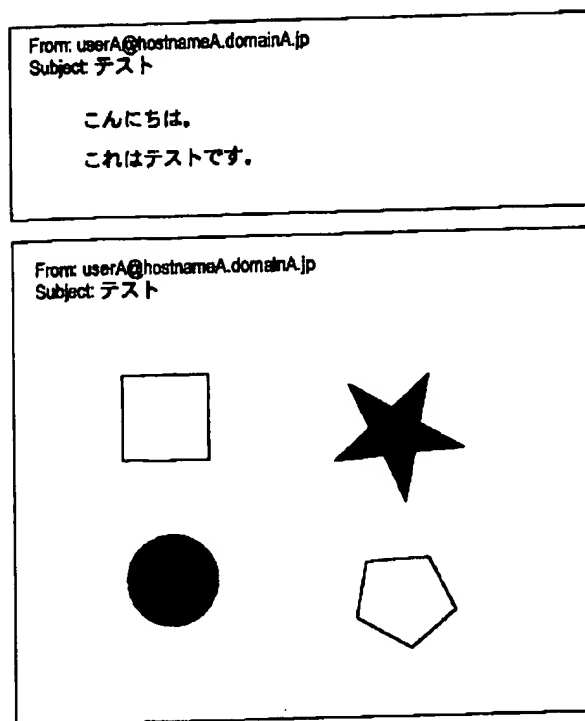


図 5

[Drawing 8]

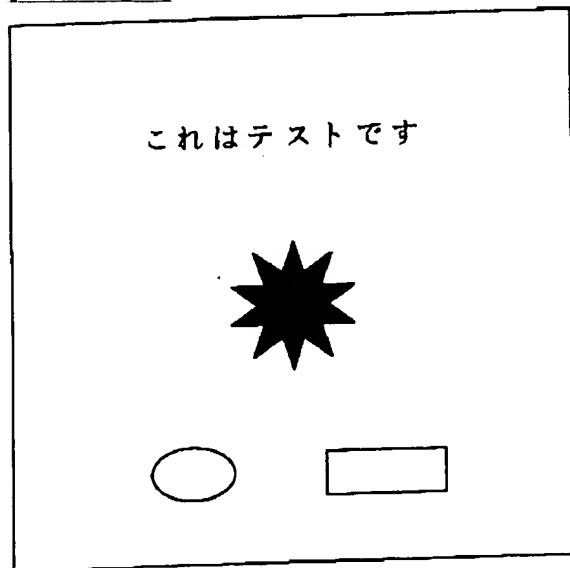


図 8

[Drawing 7]

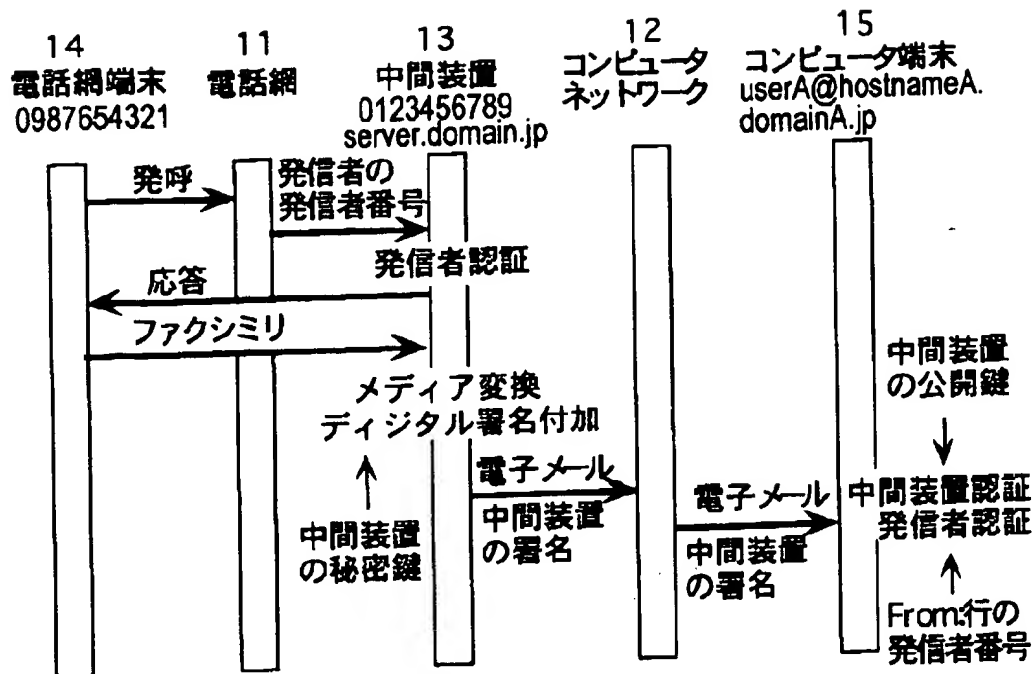


図7

[Drawing 9]

```

61 From: 0987654321@server.domainA.jp
62 MIME-Version: 1.0
63 To: userA@hostnameA.domain.jp
64 Subject: FAX
65 Content-Type: multipart/mixed; boundary=".....742959F6218E"

```

```

68 .....742959F6218E
71 Content-Type: image/gif; name="sample.gif"
72 Content-Transfer-Encoding: base64

```

```

73 {
  R01G0DdhWAgCIAAP//wAAACwAAAAAwAagCAAC4SPqcVtD6
  OctNqLs968+ww+G4kiW6ommm8sq27gvH8kzX9o3n+s73/g8MCofEovG
  ITCqXzKbzCY1SAqEZVYrNardcF/ULk7FkuuD7ACrw2IF+b2s82JOf
  lgv3f3fPw9DpEXVZen8fYmh5ih2KHx9wqZKSfYAAkdxZRUW15Seh
  o8OkW
  <中略>
  8mRRNmXnfyYoVGvd8mVhVfjNWZptmZi9mZdNmd1dmd5md99
  me8NqRohXZaibZqfZokTZp1XZpmBZpnfZpoTZapXZqqbZqrZqs
  TZtXZrubZrvZrwTZaxXZsybZszZs0Tz1XZt2bZt3Zt4TZu5XZu6b
  Zu7Zu8TZv8XZv++bZv/fZvATdwbXdwCbdwDfdwETdxFdxGbdxEl
  dxITdyJXdyKbdyLfdyMTdzNXdzObdzPfdzQTdORXd0Sbd0Tfd0UTd
  1VXdJg6AAAAA7
  .....742959F6218E .....
74

```

図9

[Drawing 13]

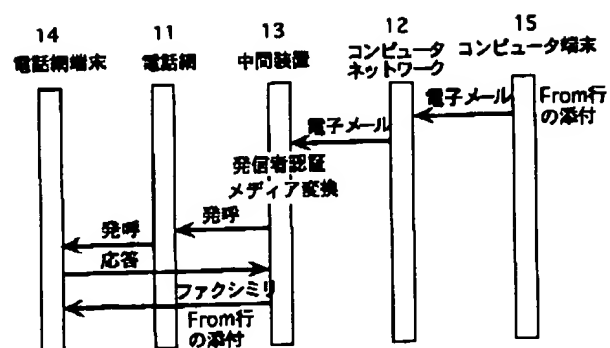


図13

[Drawing 14]

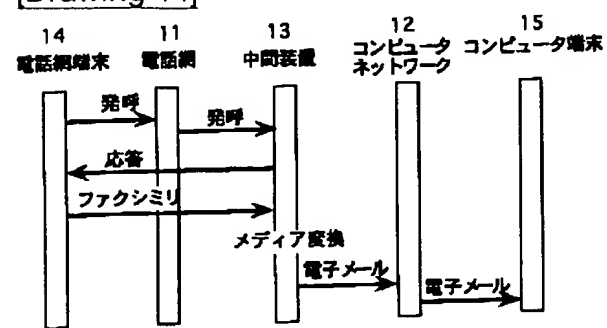


図14

[Drawing 10]

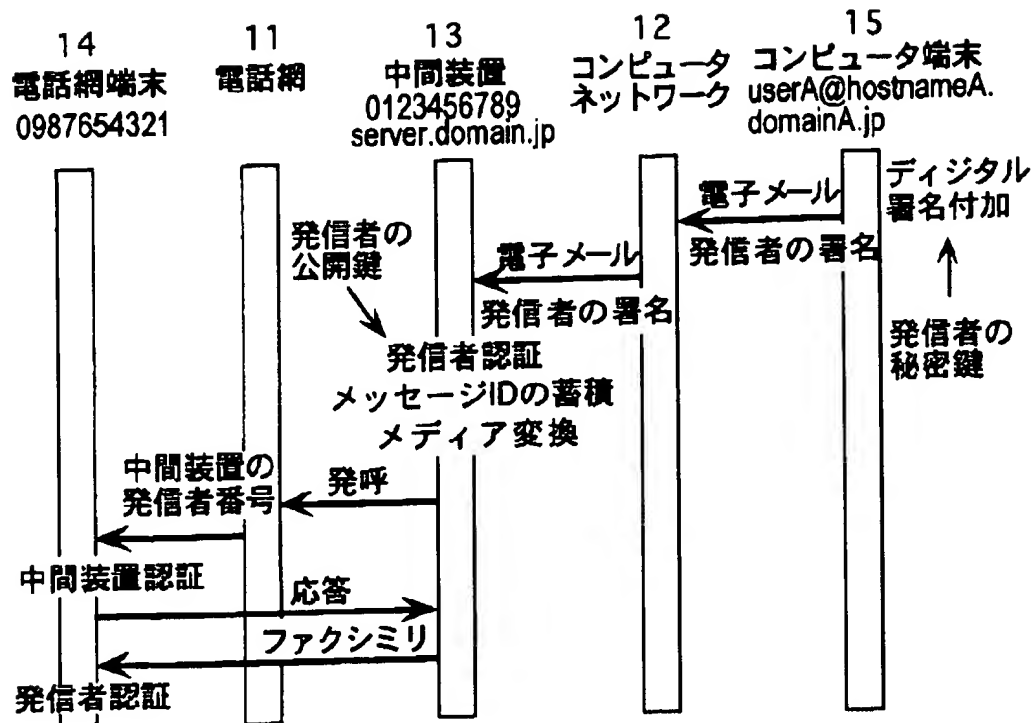


図 10

[Drawing 15]

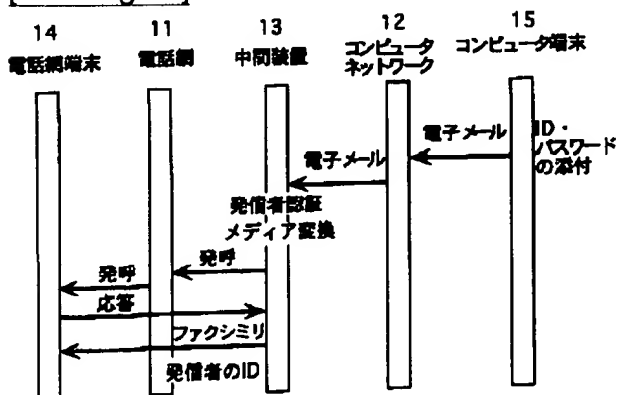


図15

[Drawing 16]

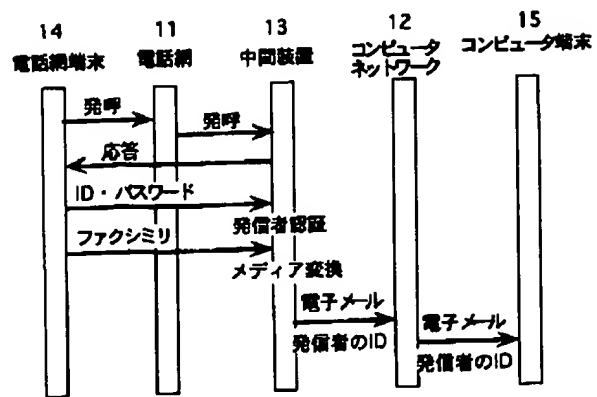


図16

[Drawing 11]

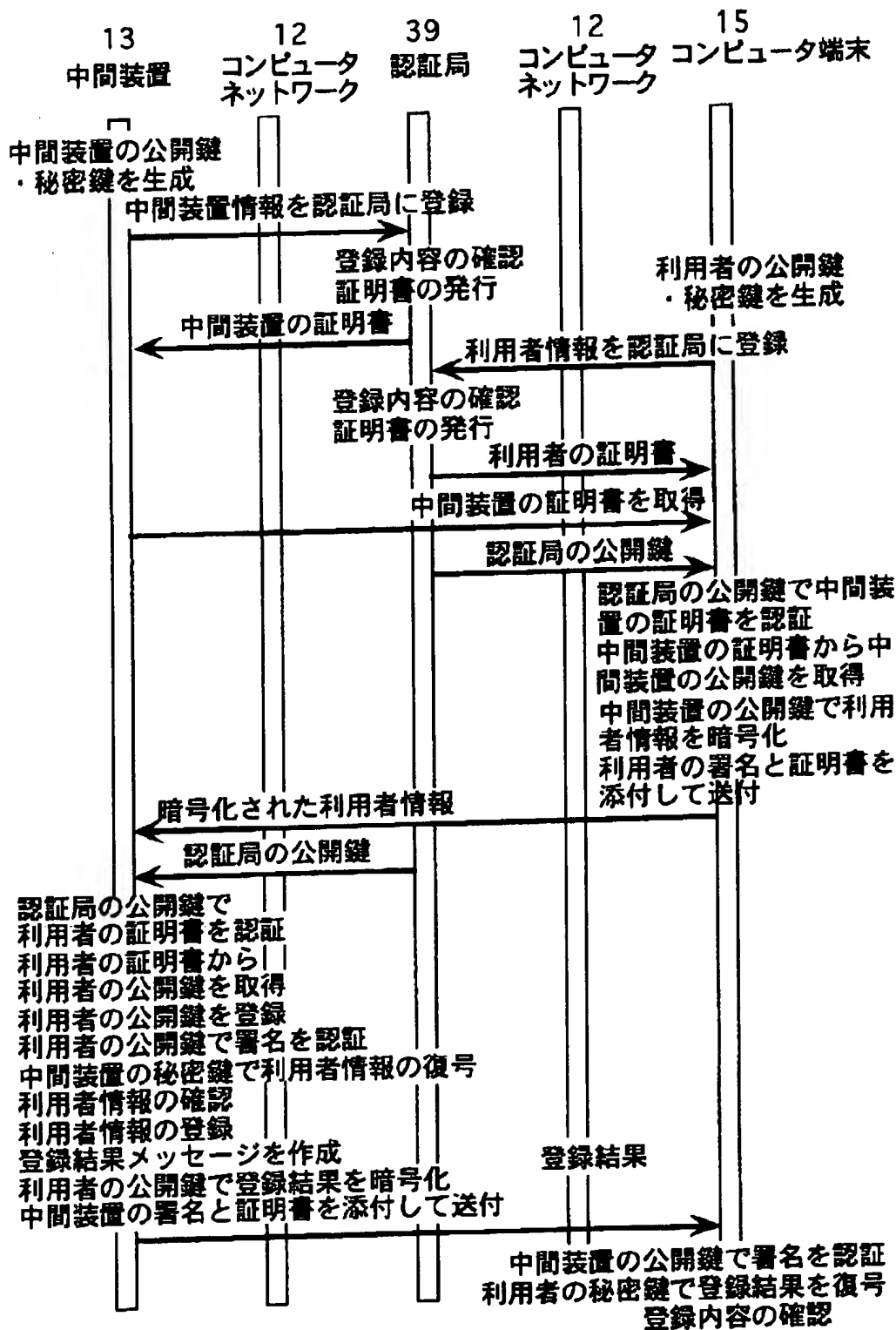


図11

[Translation done.]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-247949

(43) 公開日 平成10年(1998) 9月14日

(51) Int.Cl. ⁸	識別記号	F I
H 0 4 L 12/66		H 0 4 L 11/20 B
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00 6 4 0 B
H 0 4 L 9/32		H 0 4 M 3/00 B
H 0 4 M 3/00		11/00 3 0 3
11/00	3 0 3	H 0 4 N 1/00 1 0 7 A

審査請求 未請求 請求項の数 7 O L (全 13 頁) 最終頁に続く

(21) 出願番号 特願平9-50137

(22) 出願日 平成9年(1997) 3月5日

(71) 出願人 000004226

日本電信電話株式会社

東京都新宿区西新宿三丁目19番2号

(72) 発明者 山田 智広

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72) 発明者 高橋 勇

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72) 発明者 鈴木 晃

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(74) 代理人 弁理士 草野 卓

(54) 【発明の名称】 発信者認証方法

(57) 【要約】

【課題】 電話網端末14とコンピュータ端末15とが中間装置13を介して通信する際に発信者認証を確実に行う。

【解決手段】 端末15はメッセージにその秘密鍵によるデジタル署名を付けて中間装置13へ送信し、装置13は端末15の公開鍵で署名を検証し合格すると、メッセージをFAX画像データに変換して端末14へ送り、端末14は発信者番号を予め記憶した装置13の発信者番号と比較し、一致すればFAXを受信し、その再生画像から端末15の発信者認証を行う。

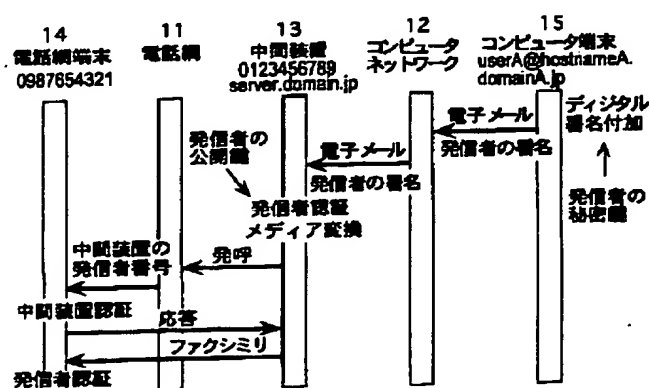


図 6

(2)

【特許請求の範囲】

【請求項1】 電話網に收容された電話網端末と、コンピュータネットワークに收容されたコンピュータ端末とが、上記電話網と上記コンピュータネットワークのそれぞれとインタフェースをもつ中間装置（以下単に中間装置と記す）を介してメッセージを通信する際の発信者を認証する方法において、

上記コンピュータ端末からメッセージを発信する際に、そのメッセージにそのコンピュータ端末を使用する発信者のデジタル署名を付けて送信し、
上記中間装置で受信したメッセージの署名を認証することを特徴とする発信者認証方法。

【請求項2】 上記中間装置の発信者番号を上記電話網端末に記憶しておき、

上記電話網端末は上記中間装置から通信要求があると、その発信者番号を上記記憶した発信者番号とを照合して中間装置の認証を行うことを特徴とする請求項1記載の発信者認証方法。

【請求項3】 上記電話網端末は、上記発信者番号の照合が合格すると、上記中間装置からメッセージと共に通知された上記コンピュータ端末の発信者情報により発信者の認証を行うことを特徴とする請求項2記載の発信者認証方法。

【請求項4】 上記中間装置に受信したメッセージのメッセージIDを記憶し、

上記コンピュータ端末はその送信メッセージにメッセージIDを与え、このメッセージIDに対しても上記デジタル署名を行い、

上記中間装置は上記コンピュータ端末からのメッセージ中のメッセージIDをそれ以前記憶した上記メッセージIDと比較し、一致すると、不正メッセージとして処理することを特徴とする請求項1乃至3の何れかに記載の発信者認証方法。

【請求項5】 電話網に收容された電話網端末と、コンピュータネットワークに收容されたコンピュータ端末とが、上記電話網と上記コンピュータネットワークのそれぞれとインタフェースをもつ中間装置（以下単に中間装置と記す）を介してメッセージを通信する際の発信者を認証する方法において、

上記中間装置は上記電話網端末より受信したメッセージを、これに対し中間装置のデジタル署名を付けて上記コンピュータ端末へ送信し、

上記コンピュータ端末は受信したメッセージの署名を認証することを特徴とする発信者認証方法。

【請求項6】 上記電話網端末の発信者番号を上記中間装置に記憶しておき、

上記中間装置は上記電話網端末からの通信要求があると、その発信者番号を上記記憶した発信者番号と照合して発信者の認証を行うことを特徴とする請求項5記載の発信者認証方法。

【請求項7】 上記メッセージの署名の認証に合格すると、上記中間装置からメッセージと共に通知された上記電話網端末の発信者情報により発信者の認証を行うことを特徴とする請求項5又は6記載の発信者認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、コンピュータネットワークと電話網の端末間で相互にメッセージ通信を行う通信における発信者の認証方法に関するものである。

【0002】

【従来の技術】図12に示すように公衆電話網11とコンピュータネットワーク12とのそれぞれにインタフェースをもつ中間装置（以下単に中間装置と記す）13が設けられ、電話網11に收容された電話網端末14とコンピュータネットワーク12に收容されたコンピュータ端末15とが中間装置13を介してメッセージを通信する通信方法が知られている。

【0003】従来、このようなコンピュータネットワーク12と電話網11の端末15、14間で相互にメッセージ通信を行うサービスでは、課金等のための発信者認証を行う方法として、目的に応じて主に次の2つの方法が取られている。第1の方法は、予め中間装置13に電子メールアドレスを登録し、コンピュータネットワーク12側からの電子メールを中間装置13を経由して電話網端末としてのファクシミリ端末14へ送信する場合は、図1に示すように、発信コンピュータ端末15から中間装置13に電子メールが送られて来ると、中間装置13は電子メール内の発信端末15のメールアドレスを予め登録した電子メールアドレスと照合することにより発信者認証を行い、その認証に合格すればコンピュータ端末15より受信した電子メール内のテキスト（文字）や画像などのメッセージをファクシミリ信号に変換し、つまりメディア変換を行って着信側へ電話網のファクシミリ端末14へ送信する。中間装置13を介してファクシミリ端末14に着信があると、ファクシミリ端末14の受信者はファクシミリ端末14の再生画像中のメッセージに添付されている前記電子メールアドレスにより発信者の確認を行う。

【0004】また、電話網端末14側からファクシミリをコンピュータ端末15に送信する場合は図2に示すように中間装置13においては、端末14から受信したファクシミリに対しては特に発信者認証を行わず、そのファクシミリ信号を電子メールの形式にメディア変換して着信側のコンピュータ端末15へ送信する。この電子メールを受信したコンピュータ端末15の受信者は端末14の発信者が付加したカバーページにより発信者の確認を行う。

【0005】第2の方法は、予め中間装置13に発信者を認証するためのID（利用者識別情報）とパスワード

(3)

3

を登録し、コンピュータネットワーク12側からの電子メールを中間装置13を経由して電話網11のファクシミリ端末14に送信する場合は、図3に示すように、発信コンピュータ端末15で発信者を認証するためのIDとパスワードを電子メールに添付して、中間装置13に対して電子メールを送信し、中間装置13は受信した電子メール内のIDとパスワードを予め登録したIDとパスワードと照合することにより発信者認証を行い、認証に合格すればその電子メールのメッセージをファクシミリ信号に変換して電話網のファクシミリ端末14に送信する。ファクシミリ端末14の受信者はファクシミリ端末14の再生画像メッセージに付加されている発信者のIDにより発信者の確認を行う。

【0006】また、電話網11側からファクシミリをコンピュータ端末15へ送信する場合は、図4に示すように、発信者がPB音で発信者を認証するためのIDとパスワードをファクシミリ端末14より入力し、中間装置13はその入力されたIDとパスワードを予め登録したIDとパスワードと照合することにより発信者認証を行い、これに合格するとその後送られて来たファクシミリを電子メールに変換してコンピュータ端末15へ送信する。コンピュータ端末15の受信者は受信した電子メールのメッセージに付加されている発信者IDにより発信者の確認を行う。

【0007】

【発明が解決しようとする課題】従来の第1の方法では、発信者の電子メールアドレスが漏洩した場合、第3者が不正に発信者の電子メールアドレスを偽装してメッセージの送信を行うことが可能であり、発信者および受信者に不利益になる場合がある。また、発信者が送信したメッセージを第3者が不正に改ざんし、発信者および受信者に不利益になる場合があるという問題点があった。更に、電話網11からファクシミリをコンピュータ端末へ送信する際には中間装置13で認証を行わないため、第3者が不正にファクシミリを送信することにより、中間装置13の管理者に不利益をもたらすおそれがあり、また、発信者が特定できないメッセージが受信者に送信されることにより、受信者の不利益になるおそれがあるという問題点があった。

【0008】従来の第2の方法では、従来の第1の方法と同様に、第3者が不正に発信者のIDとパスワードを偽装しメッセージの送信を行うことが可能であり、発信者および受信者に不利益になる場合がある。また、発信者が送信したメッセージを第3者が不正に改ざんし、発信者および受信者に不利益になる場合があるという問題点があった。更に、電話網11からファクシミリをコンピュータ端末15へ追信する際にも、第3者が不正に発信者のIDとパスワードを偽装使用してメッセージの送信を行うことが可能であり、発信者および受信者に不利益になる場合があるという問題点があった。

4

【0009】この発明は、第3者が発信者になりすまし、あるいは第3者がメッセージを改ざんすることにより発信者および受信者の不利益になるという問題点および第3者が不正にファクシミリを送信することにより中間装置の管理者の不利益になるという問題点を解決した、発信者認証方法を提案することを目的とする。

【0010】

【課題を解決するための手段】この発明は、コンピュータ端末より発信する場合はデジタル署名を行い、中間装置でメッセージに付加されたデジタル署名を使用して発信者認証を行うことで、第3者によるなりすましの防止およびメッセージに対する改ざんの検出を可能とし、電話網端末よりの発信に対しては電話網より通知される発信者番号を使用して発信者認証を行うことで、第3者によるなりすましの防止を可能とし、電話網端末に着信があると、その受信者は中間装置13より通知される中間装置の発信者番号および受信メッセージ中の発信者情報を使用して発信者認証を行うことにより発信者の確認を可能とし、コンピュータ端末に着信があるとその受信者は受信メッセージに付加された中間装置のデジタル署名を使用して中間装置の認証を行い、メッセージ内の発信者情報を取り出すことで、発信者の確認を可能とする。

【0011】

【作用】中間装置での認証において、コンピュータネットワークに接続されている発信者に対しては、メッセージに付加されたデジタル署名を使用して発信者認証を行うことで、第3者が発信者の電子メールアドレスを偽ったとしても、デジタル署名が異なれば、不正なメッセージとして破棄することができる。また、デジタル署名は発信者のみが作成できかつメッセージ毎に異なる為、第3者が不正にデジタル署名を複製した場合およびメッセージの一部が改ざんされた場合であっても検出することが可能になる。また、電子メール装置により一意に付与されるメッセージIDに対してもデジタル署名を施すことにより、同一のメッセージIDを持つメッセージを破棄することで、メッセージ全体を不正に複製した場合であっても検出が可能となる。電話網に接続されている発信者に対しては、発信者からではなく、電話網より通知される発信者番号を使用して発信者認証を行うことで、第3者が不正に成りすますことを防ぐことが可能になる。受信者での認証においても、電話網に接続されている受信者は、予め中間装置の発信者番号のみを取得しておくことで、電話網より通知される中間装置の発信者番号およびメッセージ中の発信者情報を使用して発信者認証を行うことにより発信者の確認が可能となり、コンピュータネットワークに接続されている受信者は、予め中間装置の公開鍵のみを取得しておくことで、中間装置のデジタル署名を使用して中間装置の認証を行い、メッセージ内の発信者情報を取り出すことで、発

5

信者の確認が可能となる。

【0012】

【発明の実施の形態】

実施例1

図1Aにこの発明が適用される通信システムの一例を示し、図12と対応する部分に同一符号を付けてある。電話網11は発信者番号通知手段21を備えているものである。電話網端末14は電話網11との信号の送受を行う通信制御手段22を備え、またこの例ではファクシミリ端末の場合であり、画像入出力手段23を備え、この

発明では更に、受信メッセージから発信者番号抽出手段24、更に中間装置13の発信者番号を記憶する蓄積手段25を備えている。

【0013】中間装置13は電話網11、コンピュータネットワーク12とそれぞれ通信の送受を行う通信制御手段（インタフェース）26、27を備えている他に、この発明では、発信者番号抽出手段28、送信メッセージにデジタル署名を付加する手段29、メディア変換手段30、受信デジタル署名を照合（検証）する手段31、更に、デジタル署名、とその検証に必要な公開鍵、秘密鍵を記憶する蓄積手段32を備えている。

【0014】コンピュータ端末15はコンピュータネットワーク12との通信の送受を行う通信制御手段33、電子メールの入出力手段34を備えている他に、この発明では送信メッセージにデジタル署名を付加する手段35、受信デジタル署名を照合（検証）する手段36、デジタル署名、その検証に必要な公開鍵、秘密鍵を記憶する蓄積手段37を備えている。

【0015】この発明ではデジタル署名を利用するが、これに必要とする鍵の取得について、図2を参照して説明する。中間装置13は公開鍵と秘密鍵の対を生成して、公開鍵を、認証局39に登録すると共に秘密鍵を蓄積手段32に記憶する。コンピュータ端末15は認証局39から中間装置13の公開鍵を取得し、また公開鍵と秘密鍵の対を生成し、その公開鍵を認証局39に登録すると共に秘密鍵を蓄積手段37に記憶し、更に自己の名前などの利用者情報（ID）に対し、コンピュータ端末15の秘密鍵でデジタル署名を添付して、これを中間装置13の公開鍵で暗号化して中間装置13へ送信する。中間装置13はその受信データを中間装置13の秘密鍵で復号化し、また、認証局39からコンピュータ端末15の公開鍵を取得し、この公開鍵で前記復号化デジタル署名を検証し、合格すれば、その受信した復号化したコンピュータ端末15の利用者情報を蓄積手段32に蓄積登録し、その登録結果を示すメッセージを作成して、これに対し中間装置13の秘密鍵で署名し、その署名付登録結果メッセージをコンピュータ端末15の公開鍵で暗号化してコンピュータ端末15へ送信する。コンピュータ端末15は受信した暗号化データを秘密鍵で復号化し、その復号化された署名を中間装置13の公開鍵

(4)

6

で検証し、その登録内容を確認する。

【0016】この実施例1はコンピュータ端末15から、中間装置13を経由して、電話網端末14に対してメッセージを送信する場合である。この場合電子メール装置（コンピュータ端末）15を使用する発信者は予め、例えば図2で説明した方法により、認証に必要な情報である発信者（コンピュータ端末15）の加入者情報を中間装置13内の加入者情報蓄積手段32に登録しておき、中間装置13は発信者の認証に必要なコンピュータ端末15の公開鍵を取得し、加入者情報蓄積手段32に記憶しておく、また、電話網端末14、この実施例ではファクシミリ端末を使用する受信者は予め、中間装置13の認証に必要な中間装置13の発信者番号を情報蓄積手段22に蓄積しておく。

【0017】コンピュータ端末15からメッセージを送信する際に、メール入出力手段34によりメッセージを作成し、デジタル署名付加手段35により、前記作成したメッセージに対して、コンピュータ端末15の秘密鍵を使用し、発信者のデジタル署名を付加する。このデジタル署名を付加したメッセージは、通信制御手段33により、中間装置13に対して送信される。

【0018】中間装置13はこのメッセージを通信制御手段27より受信し、デジタル署名照合手段31により、予め蓄積手段32に蓄積されたコンピュータ端末15の公開鍵を使用して、メッセージに付加されたデジタル署名の照合を行う。照合を行った結果、デジタル署名が確かに発信者のものであり且つ、改ざんされていない場合は、正しいメッセージであると解釈し、メディア変換手段30により、電子メールの内容をファクシミリ画像に変換する。デジタル署名が不正であった場合はメッセージを破棄する。メディア変換を行ったメッセージは、通信制御手段26により、電話網端末14に対して送信される。中間装置13から電話網端末14に対する発呼があると、電話網11は発信者情報通知手段21により、中間装置13の発信者番号を受信端末14に通知する。受信端末14は発信者番号抽出手段24により発信者番号を抽出し、情報蓄積手段25に蓄積されている中間装置13の発信者番号により、中間装置13からの着呼であることを確認したのち、通信制御手段22によりファクシミリを受信を行う。受信したファクシミリの再生画像は発信者の情報が付加されている為、発信者が中間装置13に登録されている発信者であることが確認できる。

【0019】なお、コンピュータ端末15で作成する電子メールは例えば図3に示すようなものである。即ち、まず発信者アドレス61が記述され、次に以下の記述のフォーマット62（この例ではMIMEバージョン1.0）が示され、これに相手先（受信者）アドレス63が続き、更に主題64がこの例では日本語JISコードでテストであることが記述され、次に内容形式65がこの

(5)

7

例ではマルチパート／混合で境界を“・・・742959F6218E”で示し、この境界66を付けて、内容形式67がこの例ではテキスト／通常、文字はJIS規格コードであることが示され、更に内容変換符号化68がこの例では7ビット符号であることが示された後にメッセージ内容であるテキスト69が記述される。次の境界70の後に内容形式71がこの例では画像であり、そのフォーマットがgifであることが示され、その内容変換符号化72がこの例ではbase64によることが示され、次にその符号化された画像データ73が記述され、その終りに境界74が付けられる。

【0020】このメッセージに対し署名した電子メールは例えば図4に示すようになる。つまり発信アドレス61、記述フォーマット62、着信アドレス63、主題64は図3と同一であり、次の内容形式65で、マルチパート、署名付きとなり、かつ境界が“Next Part Level-1-152633”となり、署名アルゴリズムがpgp-md5であることが記述され、境界66の次の内容形式67でメッセージであることとそのフォーマットrfc822が記述された後に、図3中の全メッセージの記述75がなされ、その終りの境界76に続く内容形式77にpgp法による署名であり、その署名データ78が続く、最後に境界79が付けられている。

【0021】中間装置13内のメディア変換手段30では、この例では受信メッセージ中のテキスト（文字）69が例えば図5に示すようにファクシミリ画像のデータに変換され、また画像メッセージ73も図5に示すようにファクシミリ画像のデータに変換される。この場合、両画面の左上端部に発信者アドレスと主題とが画像データとして付け加えられる。

【0022】上述した実施例の処理の流れを図6に示す。コンピュータ端末15では作成したメッセージに対し、端末15の秘密鍵で署名し、この署名付きメッセージを電子メールとして中間装置13へ送る。中間装置13は端末15の公開鍵で署名を検証し、合格すれば、そのメッセージをメディア変換して電話網端末（ファクシミリ端末）14を呼出し、端末14は中間装置13の発信者番号を確認し、正しければ、中間装置13に応答し、ファクシミリを受信する。そのファクシミリの再生画像中の発信アドレスから、その発信者、つまりコンピュータ端末15から発信されたものであることを確認する。

実施例2

図7にこの発明の実施例を示す。これは電話網端末14から中間装置13を経由して、コンピュータ端末15にメッセージを送信する場合である。

【0023】電話網端末としてのファクシミリ端末14を使用する発信者は予め、認証に必要な自分の発信者番号を中間装置13内の加入者情報蓄積手段32に登録を

8

行う。また、コンピュータ端末の電子メール装置15を使用する受信者は、中間装置13の認証に必要な中間装置の公開鍵を認証局から取得し、情報蓄積手段37に蓄積しておく。ファクシミリ端末14からコンピュータ端末15へメッセージを送信する際に、ファクシミリ入出力手段23により例えば図8に示すようなファクシミリ画像を入力する。入力されたファクシミリ画像は、通信制御手段22により、中間装置13に対して送信される。その際に端末14から中間装置13に対して発呼があると、電話網11は発信者情報通知手段21により、発信端末14の発信者番号を中間装置13に通知する。中間装置13は、発信者番号抽出手段28により、発信端末の発信者番号を抽出した後、加入者情報蓄積手段32に蓄積されている端末14の発信者番号と照合する。照合した結果が正しい場合は通信制御手段26により、ファクシミリの受信を行う。発信者番号が一致しない場合は不正な着呼と判断し、受信を行わない。受信したファクシミリ画像は、メディア変換手段30により例えば図9に示すような電子メールのフォーマットに変換する。この電子メールは図3の場合と同様に、発信アドレス61、記述フォーマット62、受信アドレス63、主題64（この例ではFAX）であり、内容形式65が記述された後の境界66の次は図3中の画像メッセージ部分と対応したものが続く。

【0024】この電子メールフォーマットに変換されたメッセージは、デジタル署名付加手段29により、図4に示した場合と同様に中間装置13のデジタル署名を付加する。デジタル署名を付加したメッセージは、通信制御手段27によりコンピュータ端末（電子メール装置）15に送信される。コンピュータ端末15は通信制御手段33により、メッセージを受信した後、デジタル署名照合手段36により、情報蓄積手段37に予め取得した中間装置13の公開鍵を使用して、メッセージに付加されたデジタル署名の照合を行う。照合した結果が正しければ、その電子メール中のFrom行に記載されている発信者情報（アドレス）により、発信者が中間装置13に登録されている発信者であることが確認できる。

実施例3

この実施例は、コンピュータ端末15から中間装置13を経由して、電話網端末14に対してメッセージを送信する場合で、実施例1との違いは、発信者が作成したメッセージにのみデジタル署名を施すのではなく、コンピュータ端末15内の通信制御手段33により付加されるメッセージIDに対してもデジタル署名を施し、これにより、メッセージIDが改ざんされることがなくなり、メッセージIDにより、一意にメッセージの識別を行うことを可能とする。これを実現するため、中間装置13内に受信したメッセージIDを記憶するID蓄積手段41が図1に実線で示すように設ける。

9

【0025】この処理手順を図10に示す。実施例と同様にコンピュータ端末15の公開鍵を中間装置13に登録し、また中間装置13の発信者番号を電話網端末14の情報蓄積手段25に蓄積しておく。コンピュータ端末15からメッセージを送信する際に、入出力手段34によりメッセージを作成し、このメッセージに対して通信制御手段33により、メッセージIDを付加する。デジタル署名付加手段35により、前記メッセージに対して、自分のデジタル署名を付加して通信制御手段33により、中間装置13に対して送信する。

【0026】メッセージを受信した中間装置13は、デジタル署名照合手段31により、予め蓄積手段32に蓄積された利用者情報を使用して、メッセージに付加されたデジタル署名の照合を行う。デジタル署名が不正であった場合はメッセージを破棄する。照合を行った結果、デジタル署名が確かに発信者のものであり且つ、改ざんされていない場合は、正しいメッセージであると解釈し、次にID蓄積手段41に蓄積されている全てのメッセージIDと受信メッセージ中のメッセージIDとの比較を行う。メッセージIDが異なる場合は、メッセージ中のメッセージIDをID蓄積手段41に蓄積し、メディア変換手段30により、電子メールの内容を図5に示したようなファクシミリ画像のデータに変換する。前記メッセージIDの比較の結果、そのメッセージIDがすでに、メッセージID蓄積手段41に存在する場合は、この受信メッセージは不正に複製されたものと判断し、そのメッセージを破棄する。メディア変換を行ったメッセージは、通信制御手段26により、電話網端末14とのファクシミリ端末へ送信する。この後の処理は実施例1と同様である。

【0027】公開鍵の取得方法としては例えば図11に示すように行ってもよい。図2の場合と同様に中間装置13、コンピュータ端末15はそれぞれ公開鍵と秘密鍵の対を生成し、公開鍵と自分の情報とをそれぞれ認証局39に登録を行う。その際に登録内の確認証明書を認証局39から発行してもらい、その証明書を蓄積手段32、37にそれぞれ蓄積しておく。コンピュータ端末15はその利用者情報を中間装置13に登録するために、まず中間装置13から中間装置の証明書を取得し、また認証局39から認証局39の公開鍵を取得し、この公開鍵を用いて、取得した中間装置の証明書の認証を行い、その認証に合格すれば、その証明書から、中間装置13の公開鍵を取出し、その公開鍵でコンピュータ端末15の利用者情報を暗号化し、これに対するコンピュータ端末15の秘密情報で署名を行い、その署名付き暗号化利用者情報と、コンピュータ端末の証明書を中間装置13へ送信する。

【0028】中間装置13では、認証局39から認証局の公開鍵を受取り、この公開鍵で受信したコンピュータ端末の証明書を認証し、これに合格すれば、その証明書

(6)

10

からコンピュータ端末15の公開鍵を取出し、その公開鍵を蓄積手段32に蓄積すると共にその公開鍵で受信した暗号化利用者情報の署名を検証し、これに合格すれば、その暗号化利用者情報を中間装置13の秘密鍵で復号化し、その利用者情報の内容に間違いがないかを確認した後、利用者情報を蓄積手段32に記憶する。その登録結果メッセージをコンピュータ端末15の公開鍵で暗号化し、その暗号化登録結果を、これに対し中間装置13の署名を付け、更に中間装置の証明書も付けてコンピュータ端末15へ送る。

【0029】コンピュータ端末15は同様にして、受信登録結果の署名を中間装置の公開鍵で検証し、更に、コンピュータ端末15の秘密鍵で復号化して登録内容を確認する。このように証明書を発行してもらい、コンピュータ端末15（あるいは中間装置13）から送信するメッセージにそのコンピュータ端末15（中間装置13）の証明書を付けて送信すれば、受信した中間装置13（コンピュータ端末15）は受信した証明書からコンピュータ端末15（中間装置13）の公開鍵を得ることができる。従って中間装置13は認証局39からコンピュータ端末15の公開鍵を取得する必要はない。

【0030】

【発明の効果】以上説明したように、請求項1乃至4の発明によれば、コンピュータ端末15からのメッセージの受け付けにおいて、中間装置13で第三者によるなりすましの防止およびメッセージに対する改ざんの検出が可能となり、また、第三者によるメッセージの複製を検出することが可能となり、発信者への課金が正しく行われるという経済的効果がある。

【0031】また、請求項5乃至7の発明によれば、電話網端末14からのメッセージの受け付けにおいて、中間装置13で第三者によるなりすましの防止が可能となり、発信者への課金が正しく行われるという経済的効果がある。また、請求項2の発明によれば、受信端末における発信者認証において、予め中間装置の情報を取得しておくだけで、発信者が正しいか否かの確認が可能になるというサービス性を向上させる効果がある。

【図面の簡単な説明】

【図1】この発明方法が適用される通信システムの例を示すブロック図。

【図2】この発明に用いられる公開鍵取得方法の手順を示す図。

【図3】コンピュータ端末15で作られたメッセージの例を示す図。

【図4】コンピュータ端末15で図3のメッセージをデジタル署名した電子メールの例を示す図。

【図5】図3のメッセージをファクシミリ画像に変換した例を示す図。

【図6】請求項2の発明の実施例のシーケンスを示す図。

(7)

11

【図7】請求項5の発明の実施例のシーケンスを示す図。

【図8】送信ファクシミリ画像の例を示す図。

【図9】図8のファクシミリ画像を電子メッセージに変換した例を示す図。

【図10】請求項4の発明の実施例のシーケンスを示す図。

【図11】公開鍵取得の他の方法のシーケンスを示す図。

【図12】この発明方法が適用される通信システムの例

12

を示す図。

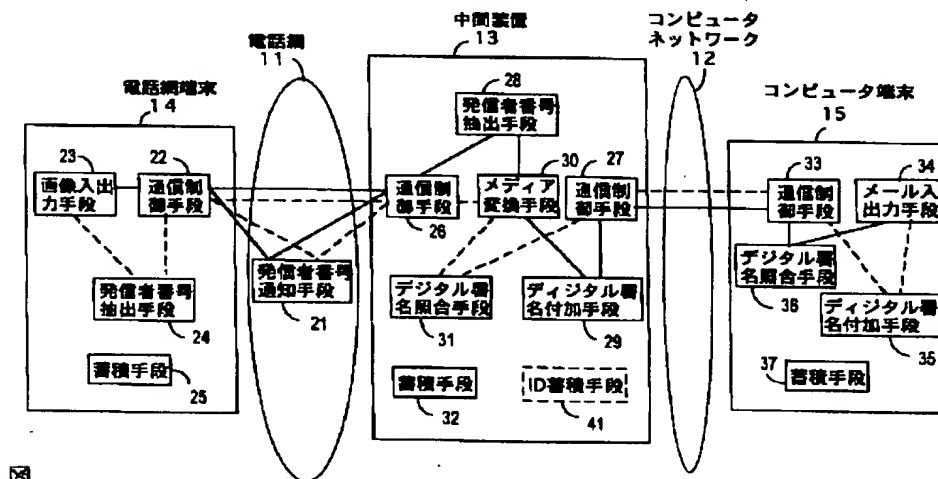
【図13】従来の電話網端末からの発信した場合のシーケンスを示す図。

【図14】従来のコンピュータ端末から発信した場合のシーケンスを示す図。

【図15】従来の電話網端末からの発信した場合のシーケンスを示す図。

【図16】従来のコンピュータ端末から発信した場合のシーケンスを示す図。

【図1】



図

【図6】

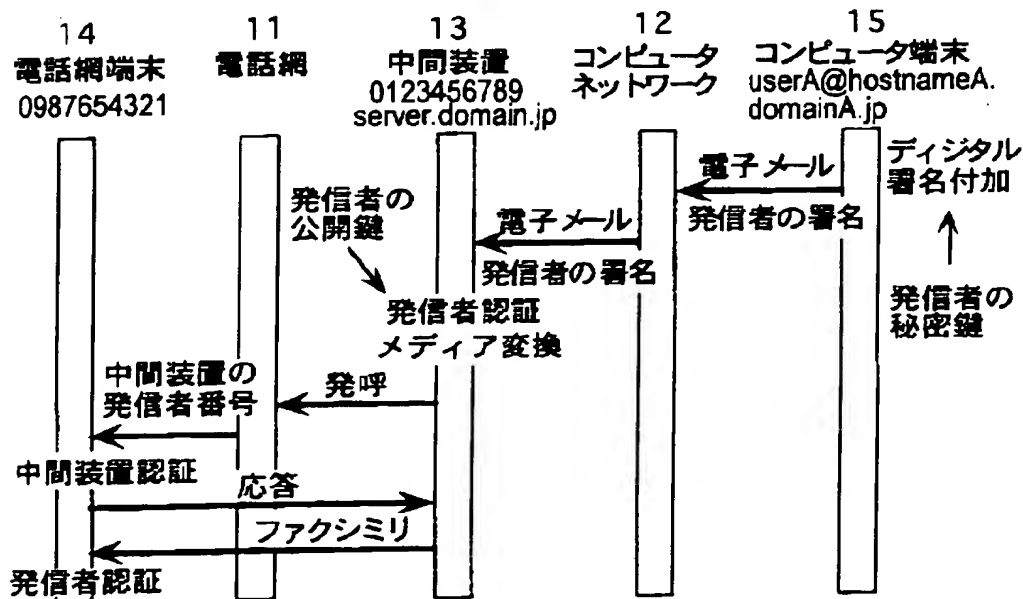


図 6

(8)

【図2】

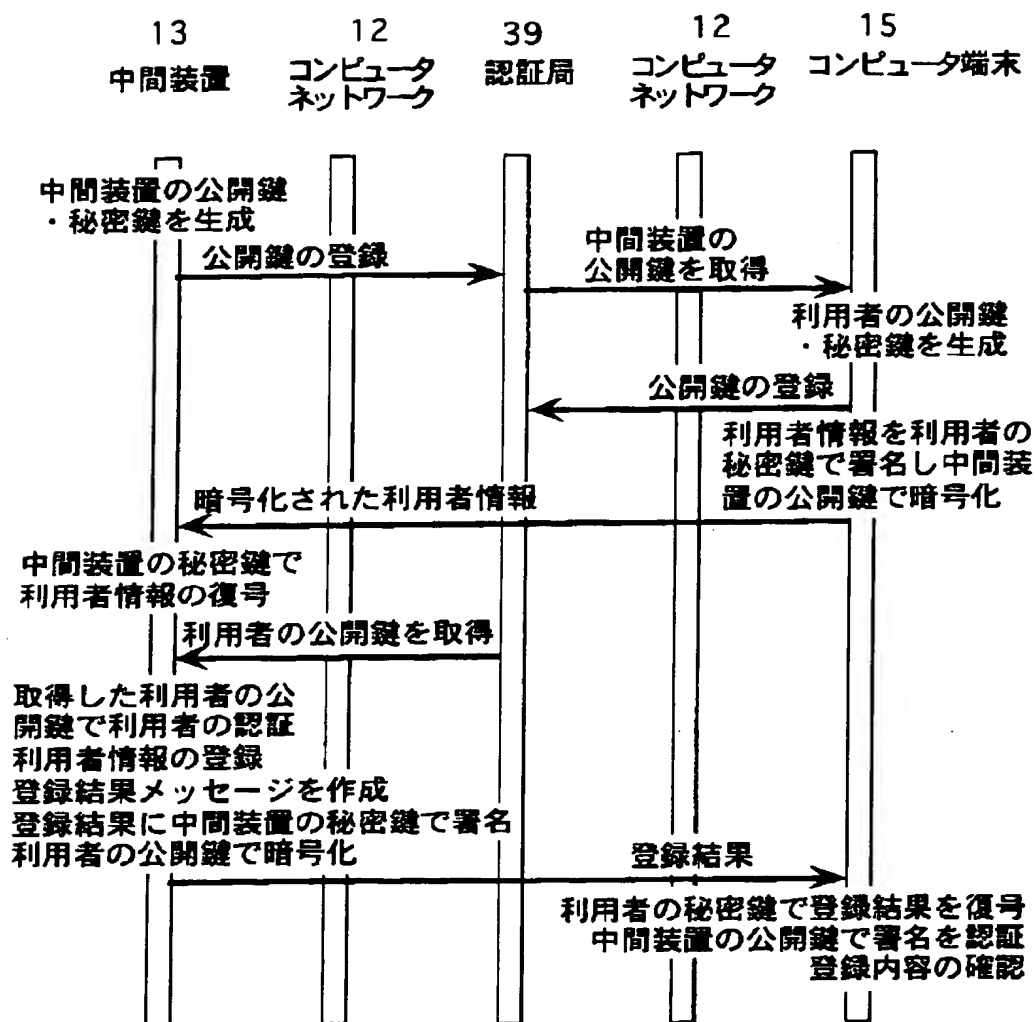


図 2

【図12】

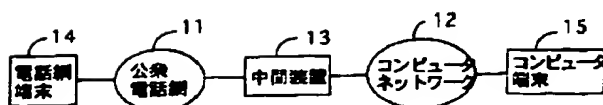


図12

(9)

【図3】

```

61 From: userA@hostnameA.domainA.jp
62 MIME-Version: 1.0
63 To: 0987654321@server.domain.jp
64 Subject: =?iso-2022-jp?B?GyRCJUyIosviGyhK?=
65 Content-Type: multipart/mixed; boundary=".....742959F6218E"

```

This is a multi-part message in MIME format.

```

66 .....742959F6218E
67 Content-Type: text/plain; charset=iso-2022-jp
68 Content-Transfer-Encoding: 7bit

```

69 こんにちは。
これはテストです。

```

70 .....742959F6218E
71 Content-Type: image/gif; name="sample.gif"
72 Content-Transfer-Encoding: base64

```

```

{
  R0KGODhwaBaAPcAAP///Hu7Ofb0vPqsDAwMXFxsG0k8uI
  KWpYWfhXJpZfpaWkA/PJawMBYVFQAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
  <中略>
  mDXSW8oSTgCv5yOtpMZVzKd9AJFFgWa8TLXa5/7EPiWpURv
  R2PhV2dC1DztZHB7PeFg78CIfg3mxUEs4vPcnZxfQdr+hy7
  byAkHXaUhdFKTKDO33JsrZU9epmWdyk4Lhryf8U58vIFg/
  kMVPFFczHMSaCDKC+MIRBYgbgRUGQX4D2QbCs92sBSzbpVm
  M07230gs8kioQ+ejzJgtBEX+QABJLkYwb98gHPvnxj4C8TUA
  AADs=
}

```

```

74 .....742959F6218E.....

```

図3

【図5】

From: userA@hostnameA.domainA.jp
Subject: テスト

こんにちは。
これはテストです。

From: userA@hostnameA.domainA.jp
Subject: テスト



【図4】

```

61 From: userA@hostnameA.domainA.jp
62 MIME-Version: 1.0
63 To: 0987654321@server.domain.jp
64 Subject: =?iso-2022-jp?B?GyRCJUyIosviGyhK?=
65 Content-Type: multipart/mixed; boundary="Next_Part_Level_1_152633";
   micalg=pgpmd5;
   protocol="application/pgp-signature"

```

```

66 .....Next_Part_Level_1_152633
67 Content-Type: message/rfc822

```

```

From: userA@hostnameA.domainA.jp
MIME-Version: 1.0
To: 0987654321@server.domain.jp
Subject: =?iso-2022-jp?B?GyRCJUyIosviGyhK?=
Content-Type: multipart/mixed; boundary=".....742959F6218E"

```

This is a multi-part message in MIME format.

```

.....742959F6218E
Content-Type: text/plain; charset=iso-2022-jp
Content-Transfer-Encoding: 7bit

```

75 こんにちは。
これはテストです。

```

.....742959F6218E
Content-Type: image/gif; name="faximage1.gif"
Content-Transfer-Encoding: base64
Content-Disposition: inline; filename="faximage1.gif"

```

```

R0KGODhwaBaAPcAAP///Hu7Ofb0vPqsDAwMXFxsG0k8uI
KWpYWfhXJpZfpaWkA/PJawMBYVFQAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
<中略>
iFgkMVPFFczHMSaCDKC+MIRBYgbgRUGQX4D2QbCs92sBSzbpVmM072
30gs8kioQ+ejzJgtBEX+QABJLkYwb98gHPvnxj4C8TUAADs=
.....742959F6218E.....

```

```

76 .....Next_Part_Level_1_1512633
77 Content-Type: application/pgp-signature

```

```

.....BEGIN PGP SIGNATURE.....
Version: 2.6.2i

```

```

78 {
  iQBVAwUBMyWlWu8FMT+s8kpAQFMCAH/dOXF1AkNPzayfthD3kpwz59z
  n6KmC2+MvJhCZhxZYxEEY4emq8gDc9jwemXnFQZ3TEYHGNHRYRTZbg=
  =g0b6
}
.....END PGP SIGNATURE.....

```

```

79 .....Next_Part_Level_1_152633-

```

図4

【図8】

これはテストです

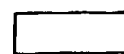


図5

図8

(10)

【図7】

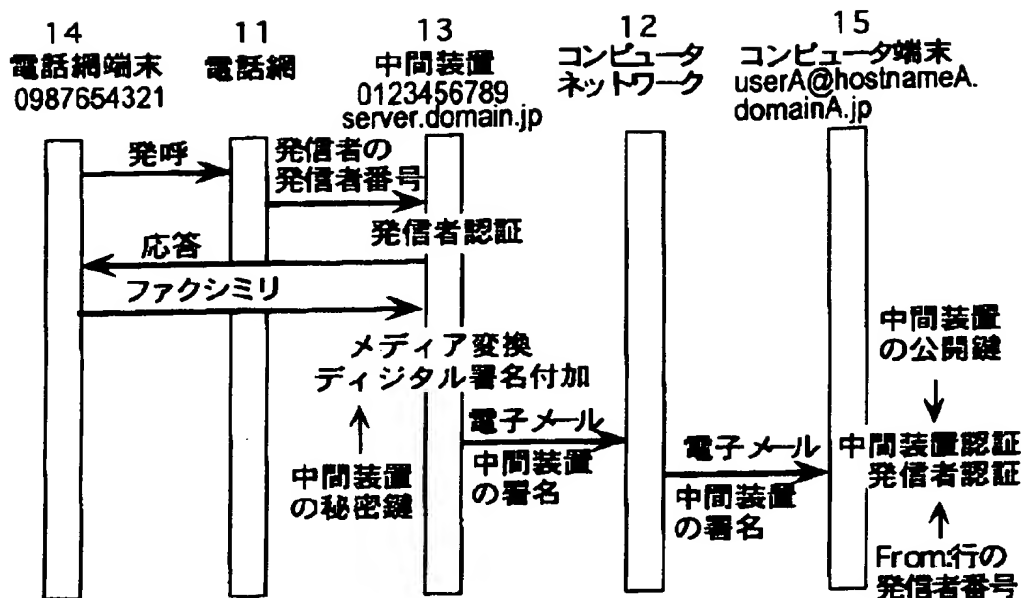


図7

【図9】

```

61 From: 0987654321@server.domainA.jp
62 MIME-Version: 1.0
63 To: userA@hostnameA.domain.jp
64 Subject: FAX
65 Content-Type: multipart/mixed; boundary=".....742959F6218E"

68 .....742959F6218E
71 Content-Type: image/gif; name="sample.gif"
72 Content-Transfer-Encoding: base64

```

```

73 {
  R01G0DdhwAagCIAAAP//wAAACwAAAAAwAagCAAC4SPqcvD6
  OctNqLs968+w+G4kiW5omm8sq27gvH8kzX9o3n+s73/g8MCofEovG
  ITCqKzKbzCY1SAqEZVYrNardcF/ULk7Fkuu07ACnw2F+tc2s82JOf
  lgv3f3Pw9DpEXVZen8Yrnh5ih2KHx9wqZKSfYAAJdxZRIW15Seh
  o8OKW
  <中略>
  9mRRNmXnrfYolVGvd8mVhVifjNWZptmZi9mZdNmd1dmd5md99
  me8NqRohXZaibZqfZokTZp1XZpmBZpnfZpoTZapXZqqbZqrZqs
  TZrtXZrubZrvTZrwTZsxXZsybZszfZs0TZ11XZ12hZ13fZ14TZu5XZu6b
  Zu7Zu8TZv9XZv+bZv/TZvATdwBXdwCbdwDfdwETdxFdxGbdxf
  dxITdyJXdyKbdyLfdyMTdzNXdzObdzPfdzQTd0RXd0Sbd0Tfd0UTd
  1VXdIg6AAAAA7
  .....742959F6218E....
74 .....742959F6218E....

```

図9

【図13】

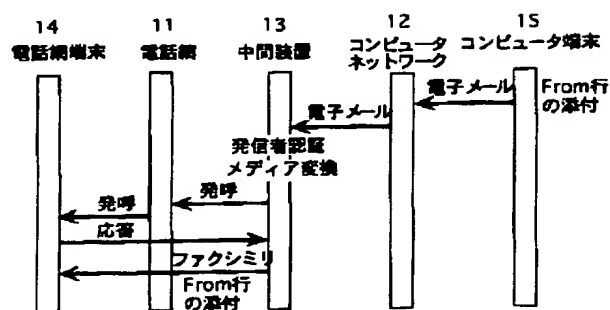


図13

【図14】

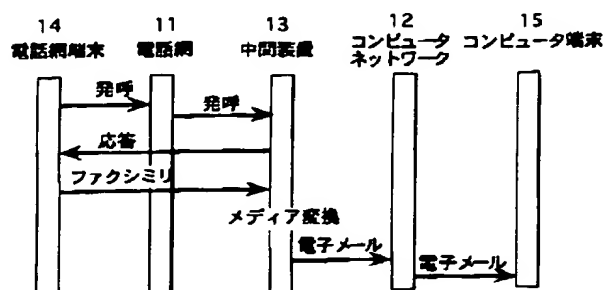
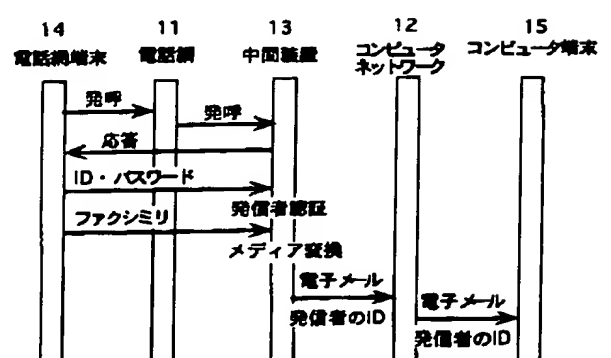
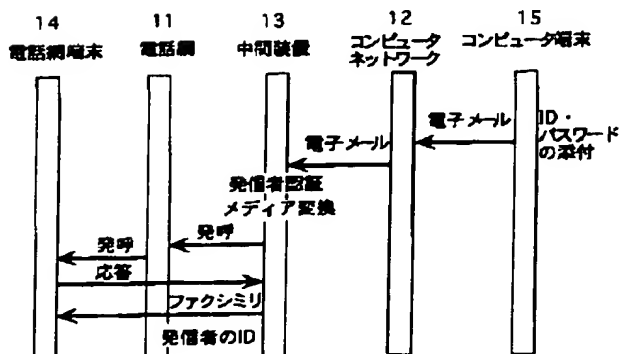
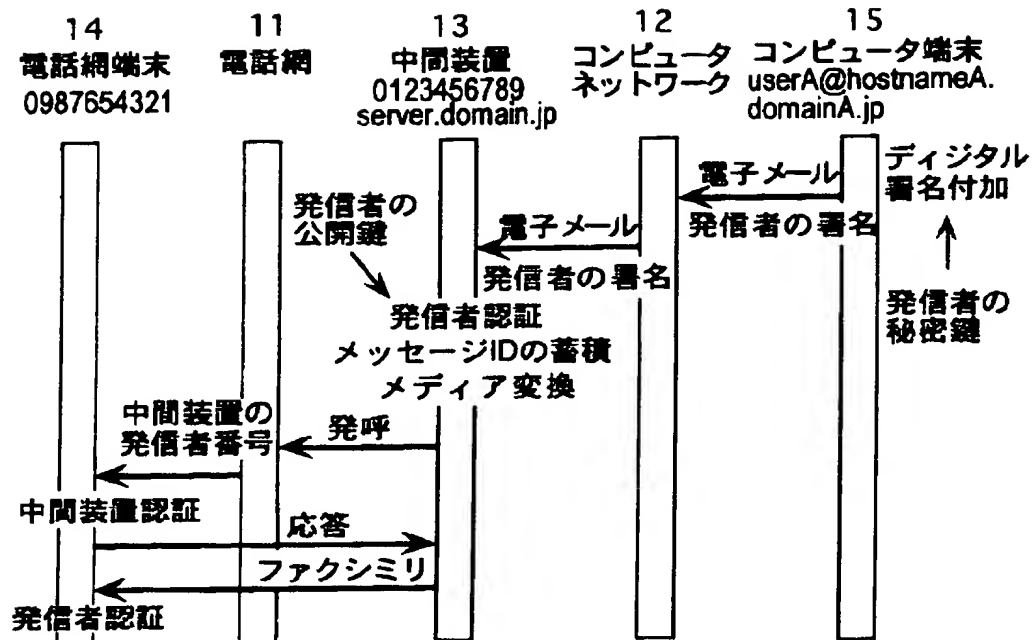


図14



(12)

【图 1 1】

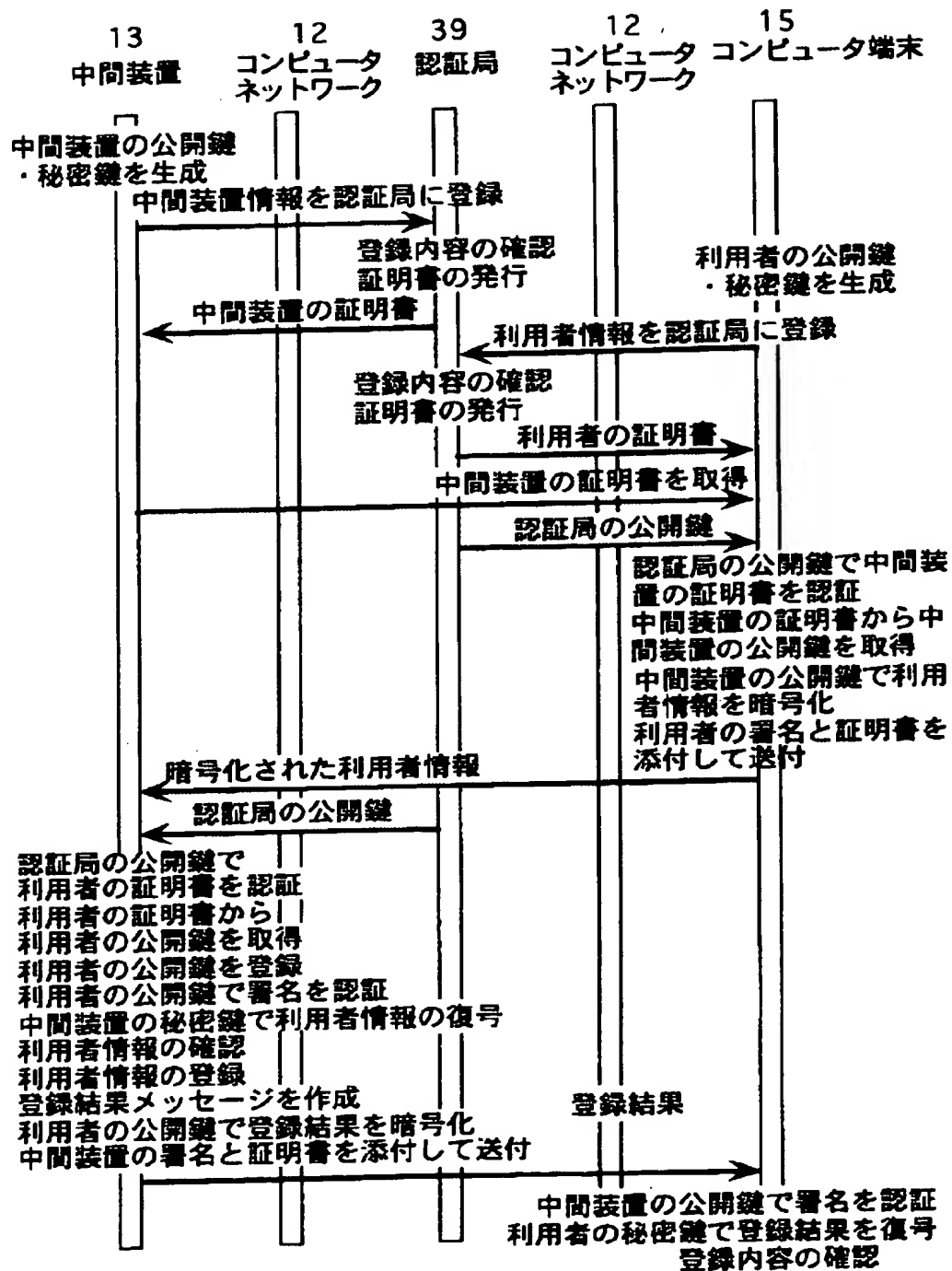


图 11

(13)

フロントページの続き

(51) Int. Cl. 6

識別記号

H O 4 N 1/00

1 0 7

F I

H O 4 N 1/32

Z

1/32

1/44

1/44

H O 4 L 9/00

6 7 5 B